Security Policy

CIS/CSE 583
What is a Security Policy?

- A document (or documents) outlining rules about who can do what to whom
  - entities (actors, objects)
  - allowed actions/relations
  - security configurations/precautions
  - practices
    - protection, detection, response
How To Define a Policy

- Identify what you are trying to protect.
- Determine what you are trying to protect it from.
- Determine how likely the threats are.
- Implement measures which will protect your assets in a cost-effective manner.
- Review the process continuously and make improvements each time a weakness is found.

What Are You Trying to Protect?

- Your private company financial or research data
  - basis of competitive advantage
- The integrity of your web server
  - critical to your business
- Your users from outsiders and each other
  - real-life example: elementary school children
What are you Protecting From?

- What, or whom?
- Theft
- Inadvertent revelation
- Denial of service
- Integrity

- Vandalism/defacement (special case of integrity)
- Hackers, terrorists, industrial espionage...

Hey, those are just variations on confidentiality, integrity, and availability!
Determine How Likely the Threats Are

- Risk assessment (attack trees)
- Consider cost of security breach
  - direct cost of data damaged/stolen
  - cost to repair
  - cost in reputation, customer trust, etc.
  - “cost” depends on the use of the system
- Prioritize risks by likelihood and cost
Implement Cost-Effective Measures

- Don’t pay more for defense than it would cost you to fix it afterwards
  - Sometimes, this can’t be defined easily
- This is the majority of what the document focuses on
  - but may or may not take the majority of the time in developing the policy
- Specify P, D, R measures
Review the Process

- Are your initial definitions still correct?
- Do the relationships between subjects and objects still hold?
- Is the security policy being implemented properly (audit)?
- If a breach occurs, review it and modify either the set of allowed actions or the security measures.
Notes on Policy

- One document, or many
- Single large document holds everything but is cumbersome
- Multiple small documents are easier to update and use, but must be kept consistent
Policy can also be Formally Specified

- Define sets: subjects (S), objects (O), actions (A)

- Write down formal rules about when subject are allowed to act on objects
  - e.g. $\forall s \in S, o \in O, a \in A$, allows(s, o, a) iff:
    - true $\Rightarrow$ no security
    - own(s, o) $\Rightarrow$ ownership
    - could include temporal relationships, etc.

- The problem comes in the implementation
Why is Policy Important?

- Without it, you have no framework to judge the security of the system.
  - If the policy accurately reflects what you want,
  - …and the system faithfully implements the policy
  - …then you’re as secure as you want to be.

- Without a written policy, you will not be secure.

- Security starts with policy definition.
Real-life Example

- Organization acted as ISP for 40+ school systems
- Also maintained computers within the systems (SW & HW)
- Wanted to “make things secure”
- Thought that they could wave a magic wand
  - firewall
  - virus filter
  - all done!
- No desire to specify policy == no security
- We walked away
Example Policy Types

- Acceptable Encryption
- **Acceptable Use**
- Analog/ISDN Lines
- Anti-Virus Process
- Audit Policy
- Dial-in Access Policy
- DMZ
- E-mail forwarding/handling policy
- Desktop security standards
- Server security standards
- Wireless network policy
Qualities of a Good Policy

- Implementable, enforceable
- Easy to understand (concise)
- Balanced between production and protection
- Explains why policy is needed
- Defines subjects, objects, relationships, actions
- Defines how violations will be handled
The Most Common Policy: AUP

- A contract between the users of the system and the owners/providers
- Says what the users are allowed to use the system for, and what they’re not
- Outlines rights of/protections provided to the users
- Describes penalty for violation
- Did you know you signed one?
Procedures

- Directions on how to comply with policy
- E.g. Policy might state that all desktop machines must use a standard configuration specified in a subdocument
- Standard specifies configuration
- Procedure tells how to configure and test system before installing
- See handout for example audit policy--note that it says nothing about procedure
Network vs. System Policies

- Most security policies do not explicitly separate the two
- Network policies: firewall configuration, DMZ rules, running services, protocols supported
- System policies: password changing, software installation (configuration), backup policy
- AUP covers both